โครงการปรับปรุงระบบเครือข่ายอินเทอร์เน็ต อาคารเฉลิมพระเกียรติ 50 พรรษา มหาวชิราลงกรณ

งานเครือข่ายและการสื่อสารสำนักคอมพิวเตอร์ ได้ดำเนินโครงการปรับปรุงระบบเครือข่ายอินเทอร์เน็ต สำหรับอาคารเฉลิมพระเกียรติ 50 พรรษา มหาวชิราลงกรณ ซึ่งในขณะนี้อยู่ระหว่างการดำเนินการติดตั้งระบบเครือข่าย คาดว่าจะดำเนินการแล้วเสร็จภายในเดือนกันยายน 2561

ตรวจประเมินคุณภาพการศึกษาภายใน

สำนักคอมพิวเตอร์รับการตรวจประเมินคุณภาพการศึกษาภายในระดับสำนัก/สถาบัน ประจำปีการศึกษา 2561 เมื่อวันที่ 6 กันยายน 2561 ณ ห้องประชุม ชั้น 2 อาคารสำนักคอมพิวเตอร์ โดยคณะกรรมการได้สรุปผลคุณภาพการศึกษาภายใน ระดับสำนัก/สถาบัน ปีการศึกษา 2561 ได้คะแนนรวม 4.71




โครงการกู้ยืมเงินซื้อคอมพิวเตอร์/กองทุนคอมพิวเตอร์

เปิดให้บุคลากรมหาวิทยาลัยยืมเงินซื้อคอมพิวเตอร์ ผ่านกองทุนคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏนครปฐม โดยผู้สมัครสามารถอ่านหลักเกณฑ์และเงื่อนไขในการกู้ยืมเงินได้ที่เว็บไซต์ของสำนักคอมพิวเตอร์ เมนูด้านบน “บริการ” >> “กองทุนคอมพิวเตอร์”

เอกสารที่ใช้ในการยืมเงินซื้อคอมพิวเตอร์

- แบบฟอร์มการยืมเงินซื้อคอมพิวเตอร์ จำนวน 1 ชุด (ดาวน์โหลดได้ที่เว็บไซต์)
- ใบรายงานเงินเดือน เดือนสุดท้ายของผู้ยืม จำนวน 1 ชุด
- สำเนาบัตรประจำตัวเจ้าหน้าที่ของรัฐ /พนักงานราชการ /พนักงานมหาวิทยาลัยของผู้ยืม จำนวน 1 ชุด
- สำเนาบัตรประจำตัวเจ้าหน้าที่ของรัฐ /พนักงานราชการ /พนักงานมหาวิทยาลัยของผู้ค้ำประกัน จำนวน 1 ชุด
- รายละเอียดคอมพิวเตอร์ ใบประกาศ/ใบเสนอราคา จำนวน 1 ชุด
- สัญญาการยืมเงิน ลงนามผู้ยืมและผู้รับเงิน จำนวน 2 ชุด
- สัญญาค้ำประกัน จำนวน 2 ชุด

ที่ปรึกษา
ผศ.ดร. นิฏฐิตา เชิดชู
ผู้อำนวยการสำนักคอมพิวเตอร์

บรรณาธิการ
อาจารย์สมพล สุขเจริญพงษ์
รองผู้อำนวยการสำนักคอมพิวเตอร์

จัดทำโดย
งานบริการวิชาการ สำนักคอมพิวเตอร์

จดหมายข่าว
สำนักคอมพิวเตอร์
มหาวิทยาลัยราชภัฏนครปฐม

cc newsletter
ปีที่ 6 ฉบับที่ 9
เดือนกันยายน 2561

facebook : cc.npru | website: http://cic.npru.ac.th

ปรับเวลาการให้บริการห้องบริการคอมพิวเตอร์และอินเทอร์เน็ต

ให้บริการ
เปิดภาคเรียน จันทร์-ศุกร์ เวลา 8.30-17.30 น. อาทิตย์ เวลา 8.30-16.30 น.
ปิดภาคเรียน จันทร์-ศุกร์ เวลา 8.30-16.30 น. อาทิตย์ เวลา 8.30-16.30 น.

ปิดบริการ
วันเสาร์ วันหยุดนักขัตฤกษ์
และวันหยุดของมหาวิทยาลัย

เริ่ม ๑ ตุลาคม ๒๕๖๑

งดให้บริการห้องฝึกอบรมคอมพิวเตอร์

เนื่องจากสำนักคอมพิวเตอร์ปรับปรุงอาคาร
ตั้งแต่เดือนกันยายน-ธันวาคม 2561
และเปิดให้บริการอีกครั้งในเดือนมกราคม 2562


ฟีเจอร์ใหม่ในอีเมล์ (Webmail)

อ่านรายละเอียดเพิ่มเติมภายในเล่ม>>

Scoop

ข่าวสารด้าน IT

การโจมตีระบบคอมพิวเตอร์ ตอนที่ ๓

โดย อ.ดร.ปิติพล พลพบู

หลังจากผู้โจมตีได้ทำการค้นหาข้อมูลที่เกี่ยวข้องกับเหยื่อด้วยวิธีการที่ผมได้กล่าวไว้ในจดหมายข่าวฉบับที่แล้ว คราวนี้ก็ถึงการโจมตีระบบจริง ๆ แล้วนะครับ โดยการโจมตีนั้นอาจเกิดขึ้นได้หลากหลายวิธี รวมถึงการใช้ Malware ที่ผมได้กล่าวถึงในจดหมายข่าวฉบับเดือนพฤศจิกายน 2560 รวมถึงข้อมูล Anti-virus application ในฉบับถัด ๆ มา นอกจากนี้ยังมีวิธีการโจมตีระบบคอมพิวเตอร์ที่เหล่าผู้โจมตีนิยมใช้กันอีกหลากหลายวิธี ผมขอยกตัวอย่างวิธีที่ค่อนข้างง่ายและนิยมใช้กันดังนี้ครับ

1. IP Spoofing เป็นเทคนิคการปลอมแปลงแหล่งที่มาของข้อมูล โดยหลอกว่าข้อมูลนั้นถูกส่งมาจากที่อื่น โดยอาศัยหลักการพื้นฐานของระบบเครือข่ายคอมพิวเตอร์ การป้องกันการโจมตีแบบนี้ขึ้นอยู่กับผู้ดูแลระบบเครือข่าย โดยจะต้องทำการตั้งค่า Firewall ให้ดี

2. Session Hijacking เป็นเทคนิคการขโมยสิทธิ์การเข้าถึงระบบจากผู้ใช้งานจริงที่ยังไม่ได้ Logout ออกจากระบบ การโจมตีนี้อาจจะทำได้ยากขึ้น หากผู้ใช้งานระบบทำการ Logout ออกจากระบบนั้น ๆ ทุกครั้งที่เลิกใช้งานหรือไม่ได้ใช้งานเป็นระยะเวลานาน

3. Denial of Service (DoS) เป็นเทคนิคการโจมตีโดยอาศัยความผิดพลาดหรือช่องโหว่ทางความปลอดภัยระบบคอมพิวเตอร์ โดยจะทำให้การทำงานของระบบนั้นหยุดชะงักหรือปิดตัวลงและไม่สามารถให้บริการหรือทำงานอื่น ๆ ต่อได้ โดยการโจมตีแบบ DoS นั้นสามารถป้องกันได้โดย Patch หรือ Update จากบริษัทผู้ผลิต Application นั้น

4. Distributed DoS (DDoS) มีจุดประสงค์เดียวกันกับ DoS เพียงแต่เปลี่ยนจากการโจมตีช่องโหว่เป็นการร้องขอเข้าใช้งานระบบอย่างถูกต้อง แต่ใช้การร้องขอจำนวนมากพร้อมกันจนกระทั่งเป้าหมายไม่สามารถรองรับการทำงานดังกล่าวได้ ทำให้ระบบเกิดความผิดพลาด หรือเป็นการกันไม่ให้ผู้ใช้งานที่แท้จริงเข้าใช้งานได้ เนื่องจากระบบทำงานถึงขีดจำกัดแล้ว การโจมตีในรูปแบบนี้ป้องกันได้ค่อนข้างยาก หรืออาจจะป้องกันไม่ได้เลย

5. Zero day attack เป็นการโจมตีในช่วงระยะแรก ๆ ที่ Hacker ค้นพบช่องโหว่ทางความปลอดภัยใหม่ ซึ่งบริษัทผู้จัดทำ Application นั้นยังไม่ทันได้จัดการหาวิธีป้องกันการโจมตีนั้น การโจมตีรูปแบบนี้จึงไม่สามารถป้องกันอะไรได้

นอกจากวิธีข้างต้นแล้ว ยังมีวิธีอื่น ๆ อีกมากมาย แล้วแต่เทคนิคที่ผู้โจมตีจะถนัดใช้งาน ซึ่งการโจมตีเหล่านี้ส่วนใหญ่จะไม่สามารถป้องกันได้โดยง่าย มักจะต้องอาศัยความรู้เกี่ยวกับระบบความปลอดภัยของคอมพิวเตอร์ระดับกลางถึงสูง แต่เราก็ยังสามารถป้องกันตัวเองได้ในระดับหนึ่งโดยการติดตั้ง Firewall และ Update ระบบปฏิบัติการและโปรแกรมต่าง ๆ ที่เราใช้งาน โดยเฉพาะกลุ่มการ Update ที่เขียนไว้ประมาณว่า Critical security issues ซึ่งจะช่วยลดช่องโหว่ทางความปลอดภัยระบบคอมพิวเตอร์ได้ไม่มากก็น้อย

บทความจาก : อาจารย์ ดร. ปิติพล พลพบู
สาขาวิชาเทคโนโลยีคอมพิวเตอร์
คณะวิทยาศาสตร์และเทคโนโลยี (2 สิงหาคม 2561)

CC newsletter

ฟีเจอร์ใหม่ในอีเมล์ (webmail) ที่น่าลองใช้

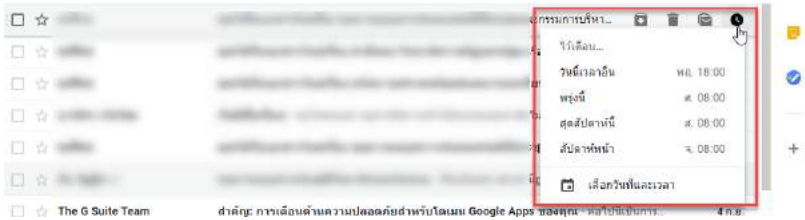
เนื่องจาก Google ได้พัฒนา Gmail เวอร์ชั่นใหม่ขึ้น ส่งผลให้อีเมล์ของมหาวิทยาลัย (webmail) ที่มีการปรับเปลี่ยนเวอร์ชั่นมีฟีเจอร์ใหม่ๆ เพิ่มเติมตามไปด้วย โดยปรับดีไซน์ให้น่าใช้งานและเพิ่มฟีเจอร์ใหม่ๆ ที่ใช้งานง่ายและมีความปลอดภัยมากยิ่งขึ้น โดยในขั้นตอนแรกผู้ใช้งานจะต้องเข้าไปที่เมนู “การตั้งค่า”  และเลือกเมนู “ลองใช้อีเมล์ของมหาวิทยาลัยราชภัฏนครปฐมใหม่” จึงจะพบกับฟีเจอร์ใหม่ๆ ดังนี้

1. Action Buttons

เพิ่มปุ่ม Action ไว้ด้านหลังหัวเรื่องอีเมล์ ผู้ใช้งานไม่จำเป็นต้องเปิดอ่านอีเมล์ก่อนก็สามารถจัดการอีเมล์ได้ โดยจะเพิ่มเมนู 4 เมนู ได้แก่ archive, delete, mark as read/unread, และเมนูใหม่ snooze

2. Snooze

ปุ่มตั้งเวลาเตือนให้ผู้ใช้งานอ่านอีเมล์ ในกรณีที่ผู้ใช้งานมีอีเมล์เข้ามาจำนวนมากๆ บางครั้งอาจจะหลงลืมอ่านอีเมล์สำคัญบางฉบับ ผู้ใช้งานสามารถตั้งค่าการเตือนให้เข้ามาอ่านอีเมล์ในช่วงเวลาที่คุณกำหนดได้



3. Nudges

ระบบเตือนอัตโนมัติเมื่อมีอีเมล์เข้ามาในกล่องจดหมายหลายวัน แต่ผู้ใช้งานยังไม่ได้ทำอะไรกับอีเมล์ฉบับนั้น ระบบจะทำการแสดงเป็น inline message ขึ้นมาถามว่าคุณจะตอบกลับหรือทำยังไงกับอีเมล์ฉบับนี้

4. Native offline

สามารถอ่านอีเมล์ย้อนหลังได้ 90 วัน โดยไม่จำเป็นต้องเชื่อมต่ออินเทอร์เน็ต